UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/068,444	02/06/2002	Giovanni M. Della-Libera	13768.1074	9546

47973 7590 05/07/2009

WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER	
HOMAYOUNMEHR, FARID	
ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
05/07/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/068,444
Filing Date: February 06, 2002
Appellant(s): DELLA-LIBERA ET AL.

Chad E. Nydegger
Reg. No. 61,020
For Appellant

SUPPLEMENTAL EXAMINER'S ANSWER

This is in response to the appeal brief filed 2/10/2009, which is the corrected version of the appeal brief filed 6/18/2007, appealing from the Office action mailed 10/13/2006.

(1) Real Party in Interest

The statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

U.S. App. 11/254,519 ("the '519 application") and U.S. App. 11/254,264 ("the '264 application") were filed on October 20, 2005 and are divisional applications of the present application. As set forth in the Appeal Brief dated January 12, 2007, Pre-Appeal Request for Reviews were filed concurrently with a Notice of Appeal for both the '519 application and the '264 application on November 13, 2006. After reviews by the Pre-Appeal Brief review panel and the Appeal Brief review panel, application '510 proceed to the Board of Patent Appeals and Interferences via an Examiner Answer dated 5/31/2007. Prosecution for the '264 application has been reopened.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Following documents were relied upon in rejection of claims:

6'678'827	Rothermel	05-1999
6'850'979	Saulpaugh	08-2000

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

10. Claims 1, 2, 3, and 5 to 19, 32 and 34 are rejected under 35 U.S.C. 102(b) as being anticipated by Rothermel (U.S. Patent No. 6678827).

10.1. As per claim 1, Rothermel is directed to a distributed security system (Fig. 1 and column 4 line 63 to column 5 line 13) comprising:

a security policy written in a security protocol independent (column 7 line 3 to 57 disclose that the Security Policy Manager Device allows a user to create a security template independent of security protocols running in NSDs. The template will be configured based on NSD protocols to create a security policy compatible with NSD, once the template is loaded on NSDs. Therefore the security policy language used at the Security Policy Manager Device must be

independent of the security protocols of NSDs) policy language (column 4line 65 to column 5 line 3), wherein the security policy is configurable to be simultaneously implemented for a plurality of computer devices within the distributed security system, wherein at least a first computer device within the distributed security system operates on an operating platform that supports at least one security protocol that is different than a security protocol supported by a platform of at least a second computer device among the plurality of computer devices (col. 13 line 30 to col. 14 line 45) wherein the first and second computer devices process the data in accordance with security policy of the distributed security system (Fig 2 and column 8 line 49 to 65).

10.2. As per claim 2, Rothermel is directed to the distributed security system of claim 1, wherein:
the security policy identifies the components of the security system (column 5 line 14 to 25).

10.3. As per claim 3, Rothermel is directed to the distributed security system of claim 1, wherein:
the security policy identifies the access rights of the security system (column 11 line 18 to 45).

10.4. As per claim 5, Rothermel is directed to the distributed security system of claim 1, wherein:

the security policy is configurable (column 7 line 25 to 37).

10.5. As per claim 6, Rothermel is directed to the distributed security system of claim 1, wherein:

the security policy language comprises at least some logic based components. As shown in Fig. 3G and column 11 line 45 to 60, the security policy creation template allows the manager to select network security information using radio buttons. Radio buttons corresponds to XOR logic. Therefore, the Examiner asserts that Rothermel policy templates include logic-based components.

10.6. As per claim 7, Rothermel is directed to the distributed security system of claim 1, wherein:

the security policy language comprises at least some rule-based components. As shown in Fig. 3D-F and column 11 line 9 to 45, the security policy creation template allows the manager to set the access rules for ping services. Therefore, the Examiner asserts that Rothermel policy templates include ruled-based components.

10.7. As per claim 8, Rothermel is directed to the distributed security system of claim 1, wherein:

the security policy language comprises procedural components. As shown in Fig. 3B and column 10 line 24 to 45, a security policy is created based on a procedure of using the policy template and completion of the policy by including network topology attributes. Therefore, the Examiner asserts that Rothermel policy templates include procedural components.

10.8. As per claim 9, Rothermel is directed to the distributed security system of claim 1, wherein:

the computer device is configured with computer-executable instructions to:

receive from the first entity a message formatted in a first protocol and transmit to second entity the message formatted in the second protocol that is different from the first protocol (Fig. 6 and column 13 line 30 to 67, and Fig 6 column 13 line 30 to column 14 line 50)

10.9. As per claim 10, Rothermel is directed to the distributed security system of claim 9, wherein:

the computer device is configured with computer-executable instructions to:

receive from the first entity a message transported with a first transport; and

transmit to second entity the message formatted in the second transport that is different from the first transport (column 16 line 48 to 62, and Fig 6 column 13 line 30 to column 14 line 50)

10.10. As per claim 11 Rothermel is directed to the distributed security system of claim 1, wherein:

the security policy is implemented in at least one application programming interface (column 13 line 42 to 67).

10.11. As per claim 12 Rothermel is directed to the distributed security system of claim 1, wherein:

the security language includes programming language constructs (column 13 line 42 to 60).

10.12. As per claim 13 Rothermel is directed to the distributed security system of claim 1, wherein:

the security policy includes an identify service (Fig. 6 item 640 and column 13 line 45 to 50).

10.13. As per claim 14, Rothermel is directed to the distributed security system of claim 1, wherein:

the security policy includes an admission service (Fig. 6 item 630, the firewall will block or admit packets)

10.14. As per claim 15 Rothermel is directed to the distributed security system of claim 1, wherein:

the security policy includes a permission service (Fig. 3d and column 11 line 9 to 15).

10.15. As per claim 16 Rothermel is directed to the distributed security system of claim 1, wherein:

the security policy includes a revocation service. As indicated in Fig. 3F, the security policy can be configured to allow or disallow a user to access a certain service, such as Ping. Changing the policy to disallow a user to continue accessing a service is analogous to revocation of a right, and therefore works as a revocation service.

10.16. As per claim 17 Rothermel is directed to the distributed security system of claim 1, wherein:

the security policy includes a mapping of entities to rights. As described in Fig. 3B and column 10 line 27 to 65, the policy is created based on security template and attributes of each entity. One of the attributes of each entity is its rights. Therefore, a policy is created based on the rights of each entity. This discloses the feature.

10.17. As per claim 18, Rothermel is directed to the distributed security system of claim 17, wherein:

the security policy further includes a mapping of entities to capabilities. As described in Fig. 3B and column 10 line 27 to 65, the policy is created based on security template and attributes of each entity. One of the attributes of each entity is its capabilities. Therefore, a policy is created based on the capabilities of each entity. This discloses the feature.

10.18 As per claim 19, Rothermel is directed to the distributed security system of claim 1, wherein:

the security policy is configured to invoke external computer-readable instructions (Fig. 6 and column 13 line 30 to 50).

Claim Rejections - 35 USC § 103

12. Claims 4, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rothermel as applied to claim 1 above, and further in view of Saulpaugh (U.S. Patent No. 6850979).

12.1 As per claim 4, Rothermel is directed to the distributed security system of claim 1, however, it does not include the specific limitation of security policy language comprises the extensible markup language. Saulpaugh teaches a method for creating message gates, useful for controlling the level of security access the

client has to the services (column 7 line 36 to 55). Saulpaugh introduces the benefits of using extensible markup language (XML) to create messages gates (column 7 line 19 to 36, column 15 line 62 to column 16 line 35).

Rothermel and Saulpaugh are analogous art because they are both related to distributed security systems and secure exchange of data between distributed network elements and devices.

At the time of invention, it would have been obvious to a skilled person in the art to improve the way that Rothermel distributes security policies between the security manager and the security devices (which in essence, is exchanging a message) using XML comprised message gates as directed by Saulpaugh.

The motivation to do so would have been to improve the security of policy exchange between the security policy manager and network security devices using a standard message exchange language that is interoperable among multiple platforms.

Therefore, it would have been obvious to use XML to create and exchange security policies.

12.2. As per claim 20, Rothermel is directed to the distributed security system of claim 19, however, it does not include the specific limitation of external computer readable instructions comprise native process code. Saulpaugh teaches a method for creating message gates, useful for invoking programs in computer native language (column 14 line 29 to 42).

Rothermel and Saulpaugh are analogous art because they are both related to distributed security systems and secure exchange of data between distributed network elements and devices.

At the time of invention, it would have been obvious to a skilled person in the art to improve the distributed security system of Rothermel to be capable of invoking programs in computer native language, as described by Saulpaugh.

The motivation to do so would have been to extend the system's range of interoperability to include systems working with machine native language.

12.3. As per claim 21, Rothermel is directed to the distributed security system of claim 19, however, it does not include the specific limitation of external computer readable instructions comprise Java code. Saulpaugh teaches a method for creating message gates, useful for invoking programs in Java code (column 14 line 29 to 42).

Rothermel and Saulpaugh are analogous art because they are both related to distributed security systems and secure exchange of data between distributed network elements and devices.

At the time of invention, it would have been obvious to a skilled person in the art to improve the distributed security system of Rothermel to be capable of invoking programs in Java code, as described by Saulpaugh.

The motivation to do so would have been to extend the system's range of interoperability to include systems working with Java code.

13. Limitations or claims 33 and 34 are substantially the same as claim 1 above.

(10) Response to Argument

In response to claim rejections based on Rothermel (US Patent No. 6'678'827), the appellant has argued that Rothermel does not teach, disclose or suggests the claim limitations. The following describes Appellant's specific arguments and the corresponding responses:

Response to appellant's argument under section titled: "A. Rothermel Does Not Teach, Disclose or Suggest the Claim Limitations" is as follows.

a. Appellant argues: "Rothermel teaches distributing a consistent security policy template to network security devices (See Col. 3, lines 33-34). While the consistent template may be configured with specific information, Rothermel does not teach or even suggest using a security protocol independent security policy language to create such a policy template or the policy itself." However, column 7 lines 3 to 57 of Rothermel discloses a Security Policy Manager Device, which allows a user to create a security policy template independent of security protocols running in Network Security Devices (NSDs). The policy template will be loaded on the NSDs, and once loaded, the template is further configured based on protocols running on the NSDs to create a security **policy** compatible with each NSD. Therefore the security policy language used at the Security Policy Manager Device must be independent of the security protocols of NSDs, otherwise it could not be configured based on different protocols running on each NSD. An example detailing how Rothermel creates a security policy for each NSD, based on an independent template is depicted in Fig. 3, and the associated text. As shown in col. 10, lines 7-24, the security policy template is first created without any regard (independent) of the specifics of devices that implement the policy. Once the policy template is distributed to each network, it is combined with the profiles of each network to create the particular policy that is deployed in each network. Note that in each network, security is enforced by NSDs, and therefore, it is the NSDs of the networks that are configured with the specific policy. It is also important to note that NSDs run different security protocols. This is shown in column 1 line 46 to column 2 line 9, where it is clearly shown that the

subject matter of Rothermel's invention is configuration of NSDs running different protocols and services. This is further depicted by Fig. 6, where the architecture of an NSD shows that NSDs work with different security protocols (see in particular item 650 of Fig. 6, showing several different security protocols such as IPSec, PPTP, etc.). Therefore, Rothermel teaches a security policy template, which is independent of the security protocols running on NSDs. The security policy template is **configured** to create the security policy running on each NSD. This configuration is based on the particulars of the security protocols running on each NSD. Therefore, Rothermel teaches a creating security policy (the security policy template), which is independent of security protocols running on devices enforcing the security. Therefore Rothermel teaches a security policy written in a security protocol independent security policy language, as required by the claimed invention.

b. Applicant further argues: "The security policy templates of Rothermel must use the existing security protocols utilized by the network security devices, thus are not equivalent to the security policy written in a security protocol independent security policy language of the independent claims 1, 33 and 34." However, col. 3 lines 33 to 34, which is cited by the Appellant reads: "*The facility allows the manager device to create a consistent security policy for the multiple NSDs by distributing a copy of a security policy template to each of the NSDs and by then configuring each copy of the template with NSD-specific information*." It is not clear how the applicant concludes that the policy templates must use the existing security protocols utilized by the network security devices. The cited

section clearly indicates that the policy templates are configured with NSD-specific information **after** they are distributed. Note that a security policy is created from a security policy template. While the security policy is configured based on NSD-specific information, the security policy **template** is independent of the NSD-specific information (protocols running on NSD), as discussed above.

Also note that the security policy is consistent as it makes each NSD process data in accordance with the general policy of the system. For example, as shown in Fig 3B and associated text, a consistent policy is created in the template. This consistent policy states: "outgoing FTP connections are allowed only from network elements defined as being within the Information Services alias". This consistent policy is to be deployed in the entire system, which comprises three different networks, running different protocols. Each network implements the policy based on specifics of their own protocols. In that sense (the details of the security protocols), the policies on different networks are different, yet they are consistent as they implement the same policy of "outgoing FTP connections are allowed only from network elements defined as being within the Information Services alias". See particularly Rothermel col. 10 lines 24-65.

c. Applicant further cited portions of their specification and argues: "This is in stark contrast to the systems disclosed in Rothermel, which does not teach, disclose or suggest simultaneous implementation across different platforms or a security policy written in a security protocol independent security policy language." However, Rothermel col. 4 line 63 to col. 5

line 13 shows that the security policy template is distributed to multiple NSDs, therefore the security policy template is simultaneously implemented across multiple NSDs. As indicated in section "a" above, NSDs support different protocols and have different configurations. This is further shown in column Fig. 1 and column 6 lines 7-25, where it is shown that NSDs support different devices, with different security policies defined for each device. Therefore, Rothermel teaches simultaneous implementation of policies for different NSDs.

It also is important to note that the claims at hand merely require the platforms support two different security protocols. In other words, the only required distinguishing factor between the two platforms is their **support** of two different security protocols. Note also that Appellant's specification does not specifically define what is meant by two different platforms. Therefore, since NSDs support different protocols, implementation of the policy across multiple NSDs meets the mentioned requirements of the claimed language.

In addition, as shown in Rothermel's Figs 3A and 3B, the security policy is implemented across different networks, indicating yet another example of Rothermel's teaching of implementing a security policy across different platforms.

As mentioned in section "a" above, Rothermel also teaches a security policy written in a security protocol independent security policy language. Therefore, Rothermel's system

teaches the requirements of the claimed invention, including simultaneous implementation across different platforms and a security policy written in a security protocol independent security policy language.

d. Appellant further cites a portion of Rothermel and argues: "Therefore, since all the devices are managed in conjunction with the LINUX OS, there is no use or motivation to even consider applying a security policy written in a security protocol independent security policy language." It appears that the appellant is arguing that Rothermel's invention is limited to NSDs running Linux OS. Otherwise there is no reason to conclude that Rothermel has no motivation to even consider applying a security policy written in a security protocol independent security policy language. However, appellant's cited portion of Rothermel refers to an example embodiment of an NSD. This is clearly shown in col. 13 line 31. In addition, Rothermel col. 14 lines 41-45 clearly shows that the Linux OS could be replaced with alternate types of software providing similar functionality. Therefore, Rothermel's invention is not limited to Linux OS. In fact, Rothermel's same exampled embodiment of Fig. 6 clearly shows NSDs consist of variety of software components and protocols, and meet the requirements of the claimed invention as mentioned in section "c" above. Note further that Rothermel column 1 line 46 to column 2 line 24 clearly shows Rothermel's motivation to support different protocols and software components across the network, as it shows that configuration of large number of different devices is indeed a requirement for successful network security management.

It is also noteworthy that item 650 of Fig. 6 shows NSDs supporting IPSec and PPTP, which use different cryptographic protocols.

e. Appellant further argues: "As stated, the LINUX OS could be replaced, however there is no specifically no mention or suggestion to combine the use of other OSs or otherwise amend the current setup discussed in relation to Fig. 6 of Rothermel for which the Office Action cites." However, Rothermel's teaching of policy implementation across different platforms is fully discussed in sections "c" and "d" above. Note that claims do not require combining different OSs.

f. Applicant further argues that Rothermel merely discloses a system for managing multiple related network security devices with a security policy template, and states: "There is no specific teaching or suggestion that the template is even written in a security protocol independent language, rather that the template is tailored towards specific devices. The Applicants cannot locate any disclaimer to this interpretation." However, as mentioned in section "a" above, the security policy template is **configured** to create the security policy running on each NSD. Also, Rothermel col. 3 lines 33 to 34 reads: "*The facility allows the manager device to create a consistent security policy for the multiple NSDs by distributing a copy of a security policy template to each of the NSDs and by then configuring each copy of the template with NSD-specific information*." This shows that the policy is specific to the NSD, but the security policy **template** is not. This is because

the template is copied to multiple different NSDs, and only after the template is configured with NSD-specific information, the specific policy is created.

Section "a" above also shows how Rothermel teaches a security policy template that is independent of the security protocols. Therefore, the security policy template is written in a security protocol independent language.

g. Appellant further cites a portion of Rothermel col. 7 lines 3-57 as follows:

When a user of the manager device desires to establish or modify a security policy for one or more NSDs such as NSDs 130 and 140, the user first selects one of the security policy templates 113 or creates a new security policy template. Security policy templates are discussed in greater detail below with respect to FIG. 3. The manager device then determines the one or more primary supervisor devices for the NSDs of interest, such as by retrieving this information from its specific security policy information 116. If this information is not stored by the manager device, the manager device can obtain the information in a variety of ways, such as by querying the NSDs of interest or by querying the various known supervisor devices.

Appellant further argues: "If the systems of Rothermel could utilize a security protocol independent language, there would be no reason to query specific supervisor devices or otherwise determine appropriate supervisor devices, because any of them could be utilized". However, the portion of Rothermel col. 7 line 3-57 cited above is followed by:

After the one or more primary supervisor devices are known, the manager device sends a single copy of the security policy template to each of the primary supervisor devices.

This clearly shows that the portion cited by the appellant is relevant to how the main manager device distributes the templates, by determining the primary supervisor devices managing the target NSDs, so that the template can be copied to them. The cited portion has no relevancy with the **content** of security policy template or whether the content is related to the specifics supervisor devices. Note that in Rothermel's system, when the main manager wants to copy the template to a group of target NSDs, it does it via supervisor devices allocated to the group of target NSDs (see Fig. 1). The supervisor devices are related to the NSDs as the gateway that manages them. For example, NSD 130 and NSD 140 are managed by a supervisor 120, and NSD 161 and NSD 162 are managed by supervisor 160 (see Fig 1). When the security template is to be copied to NSD 130 and NSD 140, the template is sent to the supervisor 120, who copies the template to said NSD 130 and 140. This is because NSD 130 and 140 are topologically connected to the supervisor 120. When the Security Policy Manager Device 110 wants to copy a template to NSD 130 and 140, it determines the supervisor managing the NSDs so the template can be sent to the managing supervisor, and eventually copied to the NSDs. Therefore, the portion cited by the appellant is relevant to the process of finding the managing supervisor so the templates could be copied (distributed) to the target NSDs. The portion of Rothermel col. 7, lines 3-57 that is relevant to the content of the policy template starts at line 25, where it states: "*Each*

NSD's copy of the security policy template can then be configured with information specific to the NSD". The content of policy template is not dependent or associated with the managing supervisor devices. As mentioned in the sections above, the security policy template will be configured to create a policy after the template is copied to multiple different NSDs. Therefore, Rothermel's security policy template is independent of the NDS-specific information and protocols, and it does teach a security policy written in a security protocol independent language as required by claims.

Response to appellant's argument under section titled: "B. The Examiner Erred in Rejecting Claims 4, 20 and 21 under 35 U.S.C. § 103(a) because They Depend from Claim 1, which Is Patentable over Rothermel as Explained above" is as follows.

Appellant argues that claims 4, 20, and 21 depend on claim 1, and because claim 1 is allowable, claims 4, 20, and 21 are also allowable. However, as discussed in the Examiner Answer dated 10/4/2007, appellant's argument relative to allowability of claim 1 is found non-persuasive. Accordingly, appellant's argument relative claims 4, 20, and 21 are also non-persuasive.

Based on the discussion above, appellant's arguments are not persuasive, and the rejections should be sustained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Respectfully submitted,

/Farid Homayounmehr/
Farid Homayounmehr
Examiner, GAU 2439

May 6, 2009

Conferees:

Kambiz Zand

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434

Michael Simitoski
/Michael J Simitoski/
Primary Examiner, Art Unit 2439